REMARKS

The Examiner has rejected Claims 1, 3-7, 9-13, 15-18, and 24-29 under 35 U.S.C. 103(a) as being unpatentable over Ranger (USPN 6,393,568) in view of Ji (USPN 5,623,600). Applicant respectfully disagrees with this rejection.

For example, the Examiner continues to rely on the following excerpt from Ranger to make a prior art showing of applicant's claimed "identifying a process for accessing files" (see Claims 1, 7, 13, and 28 et al.).

> "A computer based encryption and decryption system is disclosed which provides content analysis through a content inspection mechanism, such as detection of a computer virus using a virus detection mechanism, based on determining whether digital input information is encrypted." (see col. 2, lines 25-28)

Moreover, in the Examiner's latest Response to Arguments, the Examiner argues that "Ranger teaches the content analysis through a content inspection mechanism." Applicant respectfully disagrees with this assertion. <u>Content analysis</u> in no way meets the specificity of applicant's claimed <u>identification of a process for accessing files</u>. It appears that the Examiner is simply not taking into account the full weight of applicant's claims. Applicant does not merely analyze the content of data. Instead, applicant teaches and claims identification of a process that is used to access files, wherein <u>virus detection actions are selected based at least in part on such file-accessing process.</u>

Again, the foregoing excerpt merely suggests identifying whether a file is encrypted or not, so that the file can be decrypted prior to scanning. There is simply no disclosure, teaching or even suggestion of any sort of identification of "<u>a process for accessing files</u>," as claimed. Applicant respectfully asserts that the determination of whether a file is encrypted or not (i.e. the state of file) in no way suggests the identification of <u>a process that is accessing the file</u>. Only applicant teaches and claims a technique for <u>tailoring virus detection actions based on processes that access files</u>.

Docket: NAI1P004/00.006.01   -9-

Further in the Examiner's latest Response to Arguments, the Examiner continues by arguing that "Ji teaches identifying the process by determining whether the file is [an] executable module." Applicant respectfully disagrees with such line of reasoning. In particular, merely determining a file extension of a file (to determine whether it is executable) simply does not meet applicant's claimed identification of a process for accessing files. Any number of processes may be used to access different files regardless of file type, and Ji makes absolutely no suggestion of identifying such processes for the purpose claimed.

In response to applicant's previously-filed amendments/arguments, the Examiner now relies on the following excerpts from Ji to make a prior art showing of applicant's claimed "wherein the process is identified from a plurality of processes each carried out by an executable file, the processes including at least one process initiated by an application program selected from the group consisting of a network browser application and a word processor application, for tailoring the virus detection actions when the application program attempts to access the files" (see this or similar, but not necessarily identical, language in each of the independent claims).

"A system for detecting and eliminating viruses on a computer network includes a File Transfer Protocol (FTP) proxy server, for controlling the transfer of files and a Simple Mail Transfer Protocol (SMTP) proxy server for controlling the transfer of mail messages through the system. The FTP proxy server and SMTP proxy server run concurrently with the normal operation of the system and operate in a manner such that viruses transmitted to or from the network in files and messages are detected before transfer into or from the system. The FTP proxy server and SMTP proxy server scan all incoming and outgoing files and messages, respectively before transfer for viruses and then transfer the files and messages, only if they do not contain any viruses. A method for processing a file before transmission into or from the network includes the steps of: receiving the data transfer command and file name; transferring the file to a system node; performing virus detection on the file; determining whether the file contains any viruses; transferring the file from the system to a recipient node if the file does not contain a virus; and deleting the file if the file contains a virus." (see Abstract)

"This step is preferably performed by checking the extension of the file name. For example, .txt, .bmd, .pcx and .gif extension files indicate that the file is not likely to contain viruses while .exe, .zip, and .com extension files are of the type that often contain viruses. If the file to be transferred is not of a type that can contain viruses, then the method continues in step 612." (see col. 7, lines 35-40)

Docket: NAI1P004/00.006.01   -10-

Further, the Examiner argues that "Ji teaches determining whether the file to be transferred is of a type that can contain viruses. This step is performed by checking the extension of the file name. For example, .txt, .bmd, .pcx. and gif extension files indicate that the file is not likely to contain viruses while .exe, .zip, and .com extension files are of the type that often contain viruses."

Whether this is true or not, Ji (in combination with Ranger) simply fails to meet applicant's claims. Specifically, reviewing file extensions simply does not rise to the level of specificity of applicant's claims. Again, any number of processes can access different files of different extensions. In other words, merely reviewing a file extension does not identify a process that is accessing the file. Moreover, Ji merely makes a blanket assertion that a word processor may reside on the computer. This, in no way, suggests that it is determined when such word processor (or network browser) is accessing a file, so that virus detection actions may be tailored in response to such accessing.

Only applicant teaches and claims a technique that is capable of identifying an application program (i.e. a network browser application or a word processor application) that is attempting to access a file, and tailoring the virus detection actions in view of the access attempt by such specific application program.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck,*947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the first and third element of the *prima facie* case of obviousness has not been met. For example, with respect to the third element of the *prima facie* case of obvious, such element has not been met since the prior art references, when combined, fail to

Docket: NAI1P004/00.006.01   -11-

teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

It is further noted that the Examiner has still not even attempted to make a specific prior art showing of the subject matter of Claims 3 and 4 et al. See below:

"wherein the virus detection actions are selected by determining a category associated with the process, and selecting a set of virus detection actions based on the determined category" (see Claim 3 et al.); and

"identifying the files being accessed, and selecting the virus detection actions based at least in part on the identity of the files" (see Claim 4 et al.).

Yet again, a notice of allowance or a specific prior art showing of such claimed features, in combination with the remaining claim limitations, is respectfully requested.

Even still, the Examiner relies on the following excerpt from Ranger to make a prior art showing of applicant's claimed "wherein the process is identified by inspecting ... a file signature associated with the process." (See Claim 5 et al.)

```
"The content inspection mechanism analyzes decrypted content for such
things as virus patterns, keywords, unknown program format, clearance
labels or any other content based criteria." (col. 2, line 29)
```

The Examiner further argues that "Ranger teaches determining whether digital information is encrypted." Applicant respectfully disagrees with this assertion. The disclosure of an encryption determination in no way meets applicant's claimed file signature, let alone identifying a process accessing a file based on a file signature associated with the process. A notice of allowance or a specific prior art showing of such claimed features, in combination with the remaining claim limitations, is respectfully requested.

Docket: NAI1P004/00.006.01   -12-

Still yet, it appears that the Examiner has overlooked numerous particular limitations in previously added Claim 29. Note, for example, the emphasized limitations noted below (which are non-existent in the remaining claims).

"(a)   identifying a process for accessing files;

(b)   selecting virus detection actions based at least in part on the process; and

(c)   performing the virus detection actions on the files;

wherein the process is identified from a plurality of processes each carried out by an executable file, <u>the processes initiated by application program-related executable files including FindFast.exe, WinWord.exe, and Explorer.exe</u>, for tailoring the virus detection actions when attempts are made to access the files;

wherein the virus detection actions are selected by determining a category associated with the process, and selecting a set of virus detection actions based on the determined category;

wherein the process is identified by <u>inspecting a name of the process, a path of the process, a file signature associated with the process, a version of the process, a manufacturer of the process, a function being called during the process, an owner of the process, a name of an executable file associated with the process, a method in which files are being accessed by the process, type(s) of shared libraries used by the identified process, and a user of the process</u>" (<u>note the all-inclusive language</u>).

Again, applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest <u>all</u> of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

Docket: NAI1P004/00.006.01   -13-

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P004/00.006.01).

Respectfully submitted,
Zilka-Kotab, PC

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100

Docket: NAI1P004/00.006.01   -14-